# CLAIM AMENDMENTS

1. (currently amended) A method for facilitating secure hardware token issuance and use, said method comprising the steps of:

storing an only instance of a private key [on] within the hardware token, the hardware token being adapted to prevent the private key from being exported from the hardware token;

binding the private key to a subscriber with a digital certificate for the subscriber;

creating a contract establishing legal ownership over the physical manifestation of the private key as contained within the hardware token; and

the subscriber using the private key to create a digital signature [on the hardware token].

2. (original) The method of claim 1, wherein the hardware token is issued by a trusted entity.

3. (original) The method of claim 2, wherein the contract specifies that the physical manifestation of the private key is owned by the trusted entity.

4. (original) The method of claim 3, wherein the trusted entity is an issuing participant.

5. (original) The method of claim 1, wherein the contract specifies that the physical manifestation of the private key is owned by a root entity.

6. (original) The method of claim 1, wherein the contract specifies that the physical manifestation of the private key is owned by the subscriber.

7. (original) The method of claim 1, wherein the hardware token is a smartcard.

8. (original) The method of claim 1, wherein the hardware token is a PCMCIA device.

9. (original) The method of claim 1, wherein the private key is an identity private key.

10. (original) The method of claim 1, wherein the hardware token comprises means for monotonically counting each time the private key is used to create a digital signature.

11. (original) The method of claim 1, wherein the hardware token comprises means for permanently storing a PIN/passphrase.

12. (original) The method of claim 11, wherein the subscriber must enter the PIN/passphrase before a digital signature is generated.

13. (currently amended) The system of claim 12, wherein the subscriber must enter the PIN/passphrase each time a digital signature is generated.

14. (original) The system of claim 1, wherein the digital signature comprises security data.

15. (original) The system of claim 14, wherein the security data is signed to create a security-data cryptogram.

16. (original) The system of claim 15, wherein the security-data cryptogram is generated using an algorithm different than the one used to create the digital signature.

17. (original) The system of claim 14, wherein the security data comprises data that is the subject of the digital signature.

18-24. (canceled)